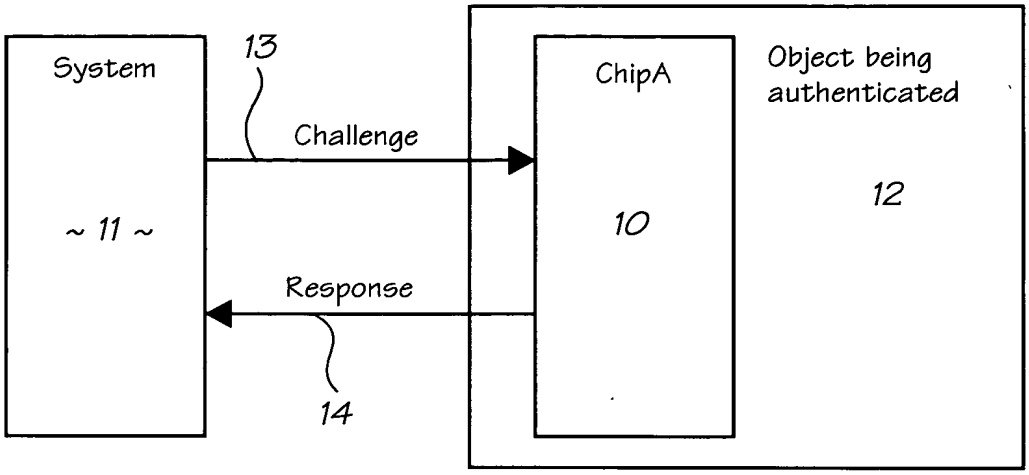
System
13
Challenge
~ 11 ~
Response
14
ChipA
10
Object being
authenticated
12

FIG. 1

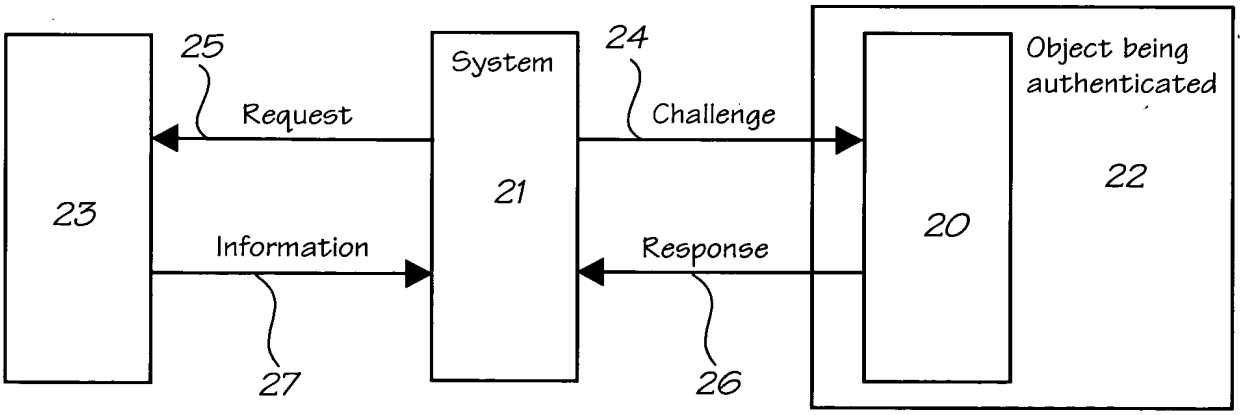
25
Request
23
Information
27
System
21
24
Challenge
Response
26
20
Object being
authenticated
22

FIG. 2

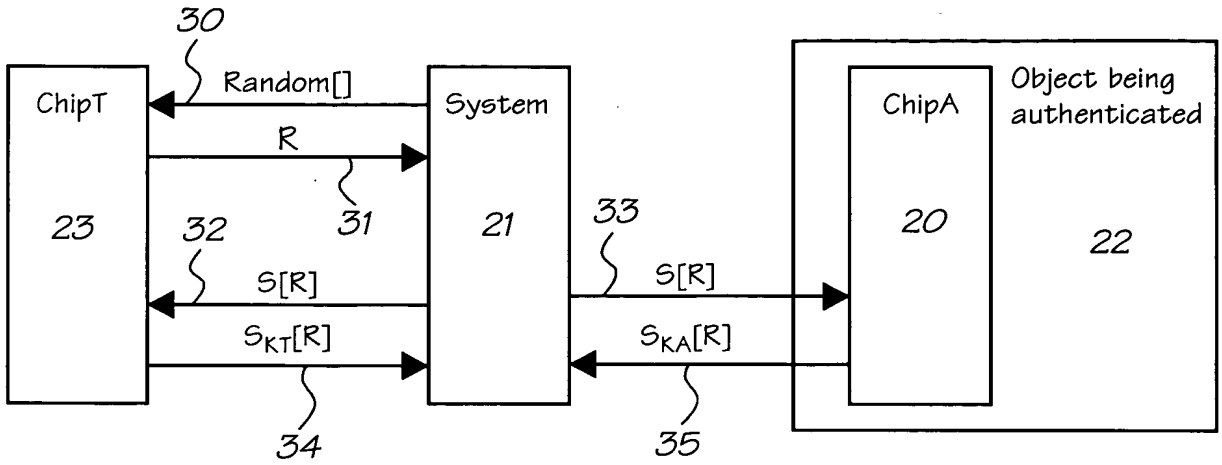
30
Random[]
ChipT
System
ChipA
Object being authenticated
R
23
31
21
20
22
32
33
S[R]
S[R]
$S_{KT}[R]$
$S_{KA}[R]$
34
35

FIG. 3

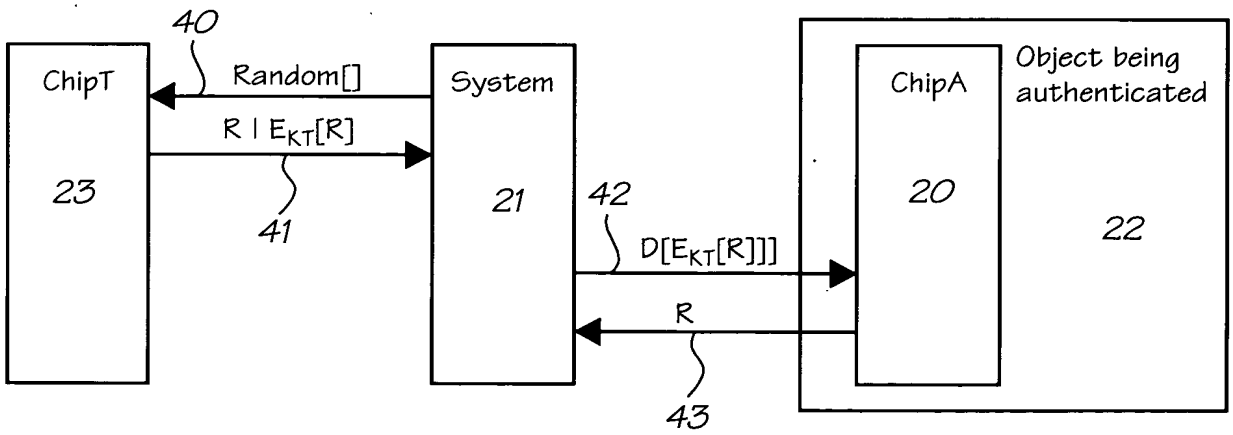
40
Random[]
ChipT
System
ChipA
Object being authenticated
$R \mid E_{KT}[R]$
23
41
21
42
20
22
$D[E_{KT}[R]]]$
R
43

FIG. 4

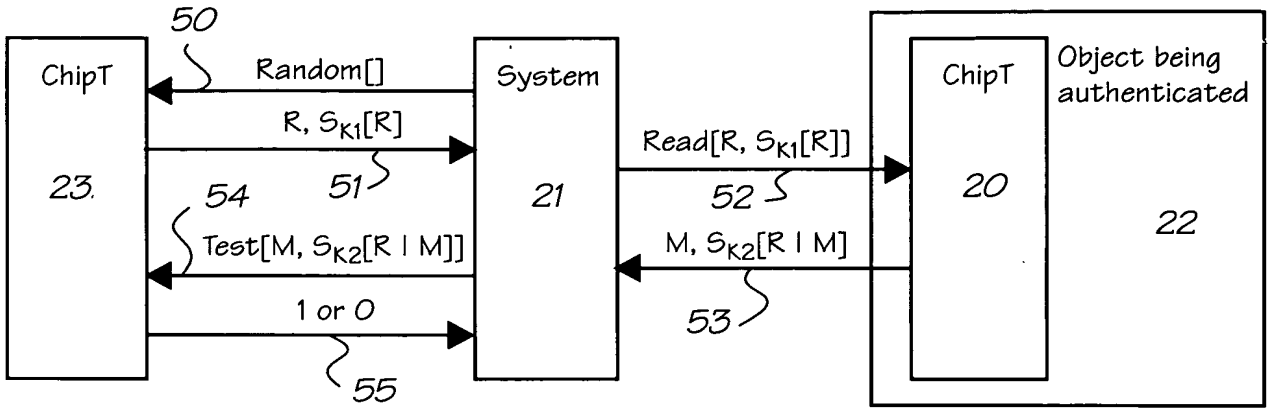
50
ChipT
Random[]
System
ChipT
Object being authenticated
R, S_{K1}[R]
Read[R, S_{K1}[R]]
23
54
51
21
52
20
22
Test[M, S_{K2}[R | M]]
M, S_{K2}[R | M]
1 or 0
53
55

FIG. 5

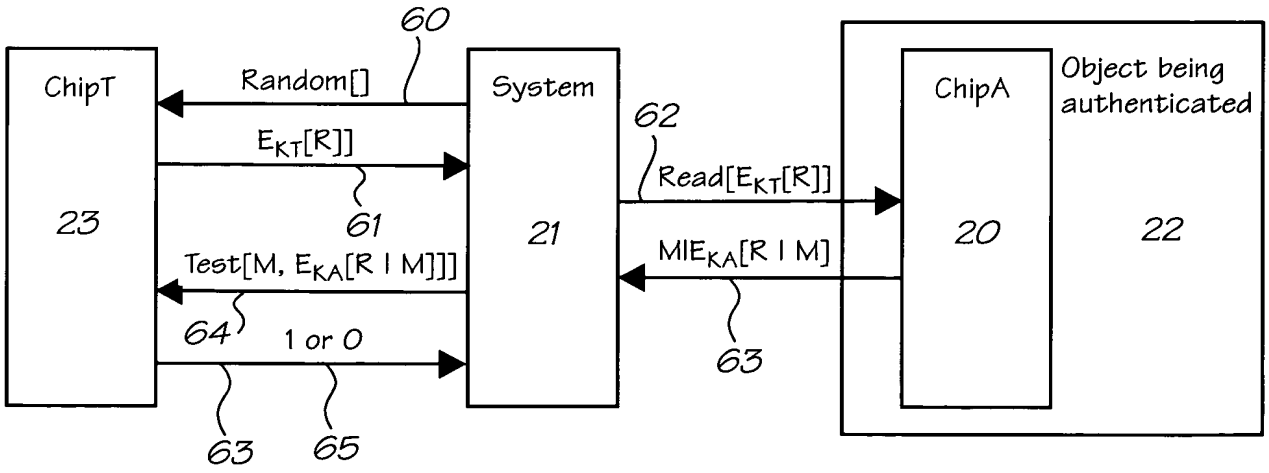
60
ChipT
Random[]
System
ChipA
Object being authenticated
62
E_{KT}[R]]
Read[E_{KT}[R]]
23
61
21
20
22
Test[M, E_{KA}[R | M]]]
MIE_{KA}[R | M]
64
1 or 0
63
63
65

FIG. 6

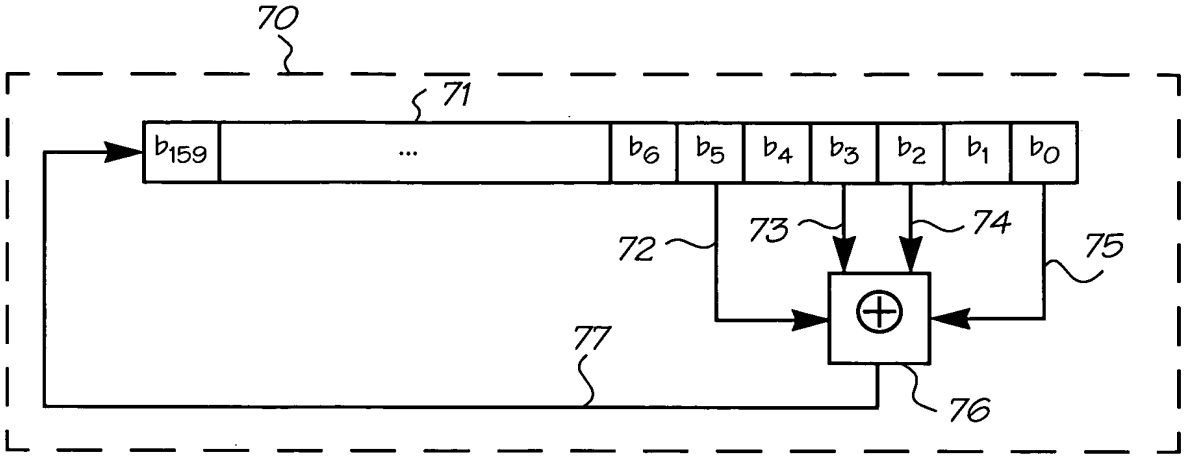

FIG. 7

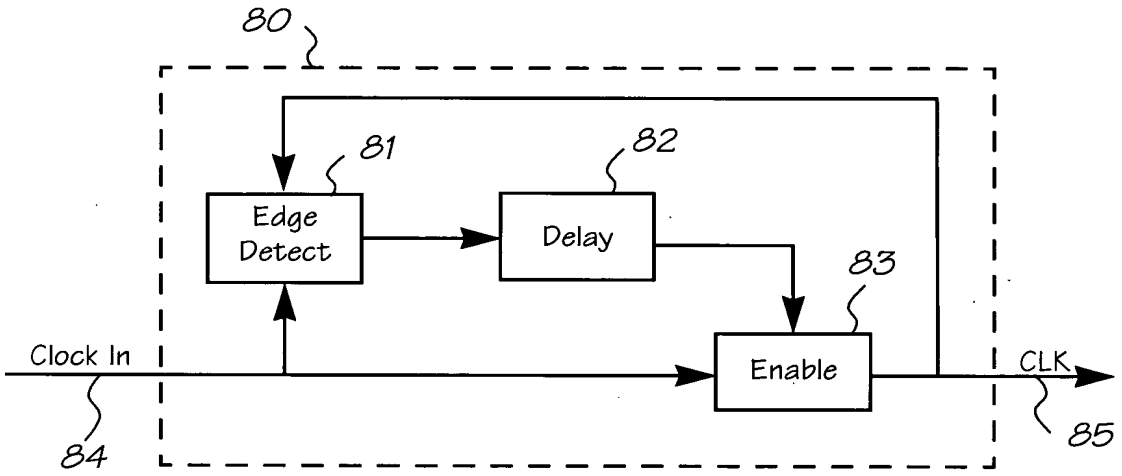

FIG. 8

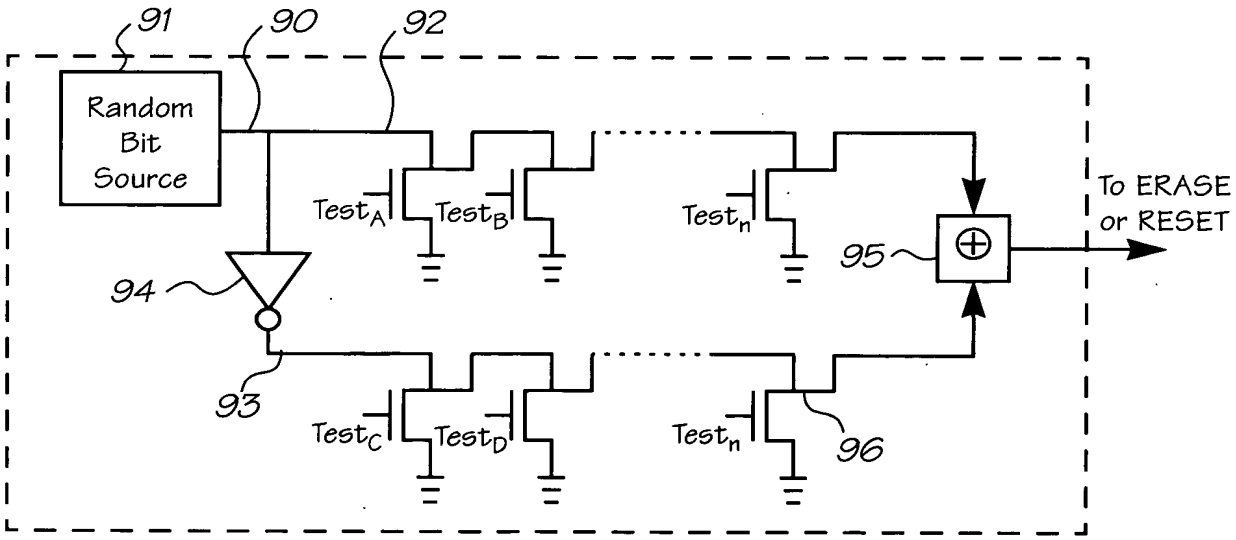

FIG. 9

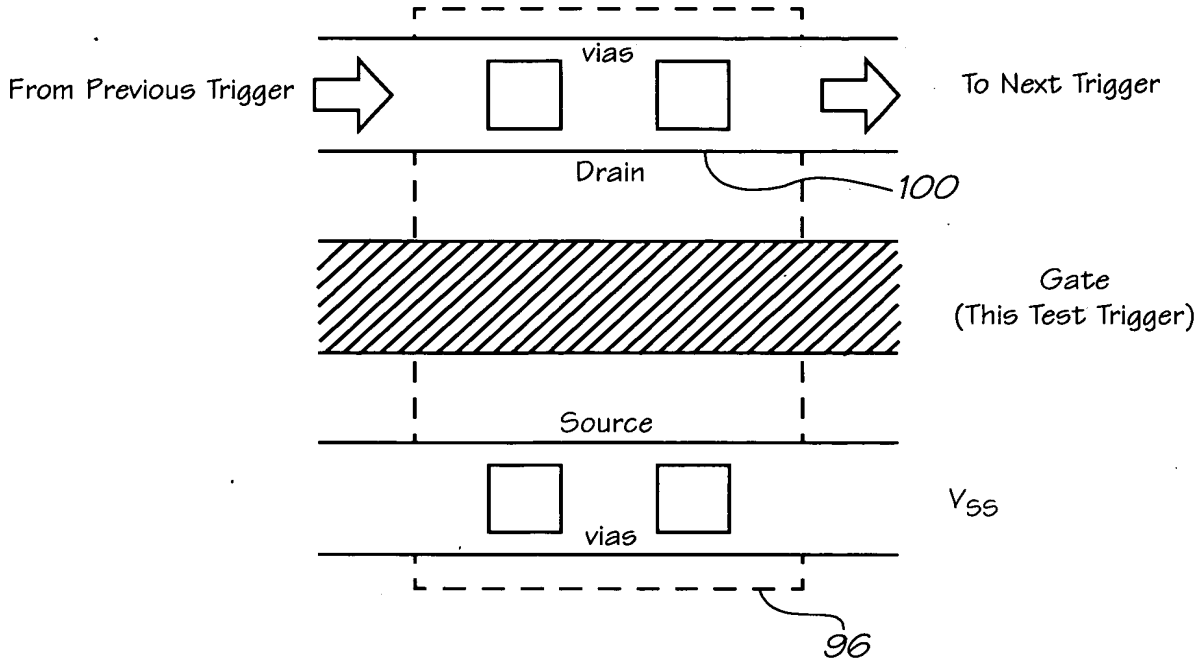
From Previous Trigger
vias
To Next Trigger
Drain
100
Gate
(This Test Trigger)
Source
V_{SS}
vias
96

FIG. 10

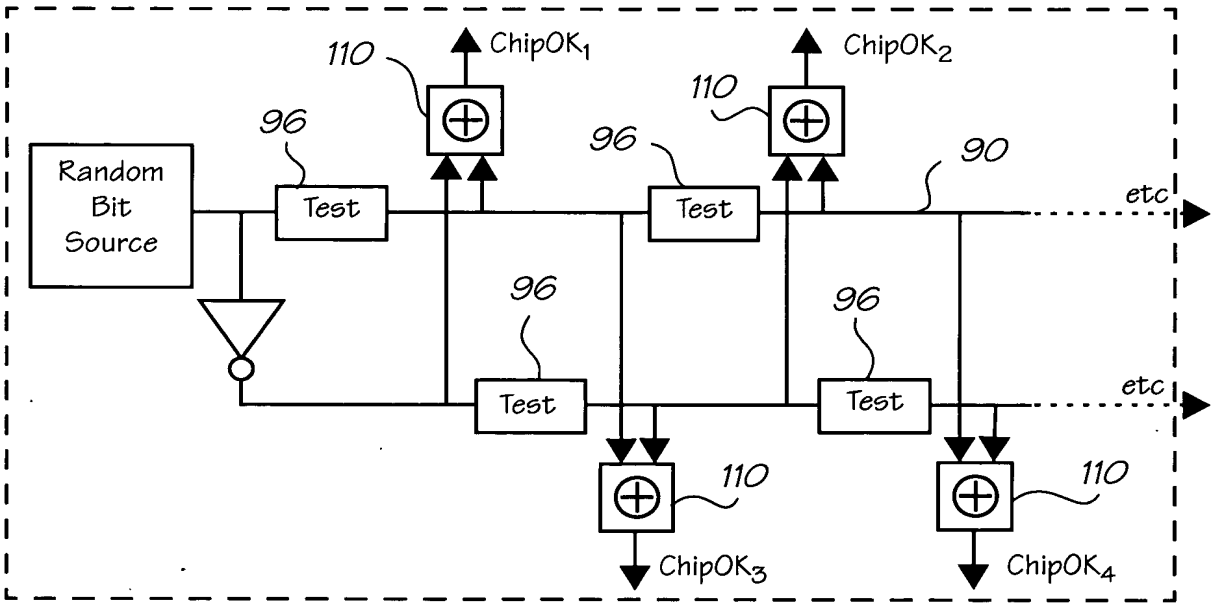
110
$ChipOK_1$
$ChipOK_2$
110
96
96
90
Random
Bit
Source
Test
Test
etc
96
96
Test
Test
etc
110
110
$ChipOK_3$
$ChipOK_4$

FIG. 11

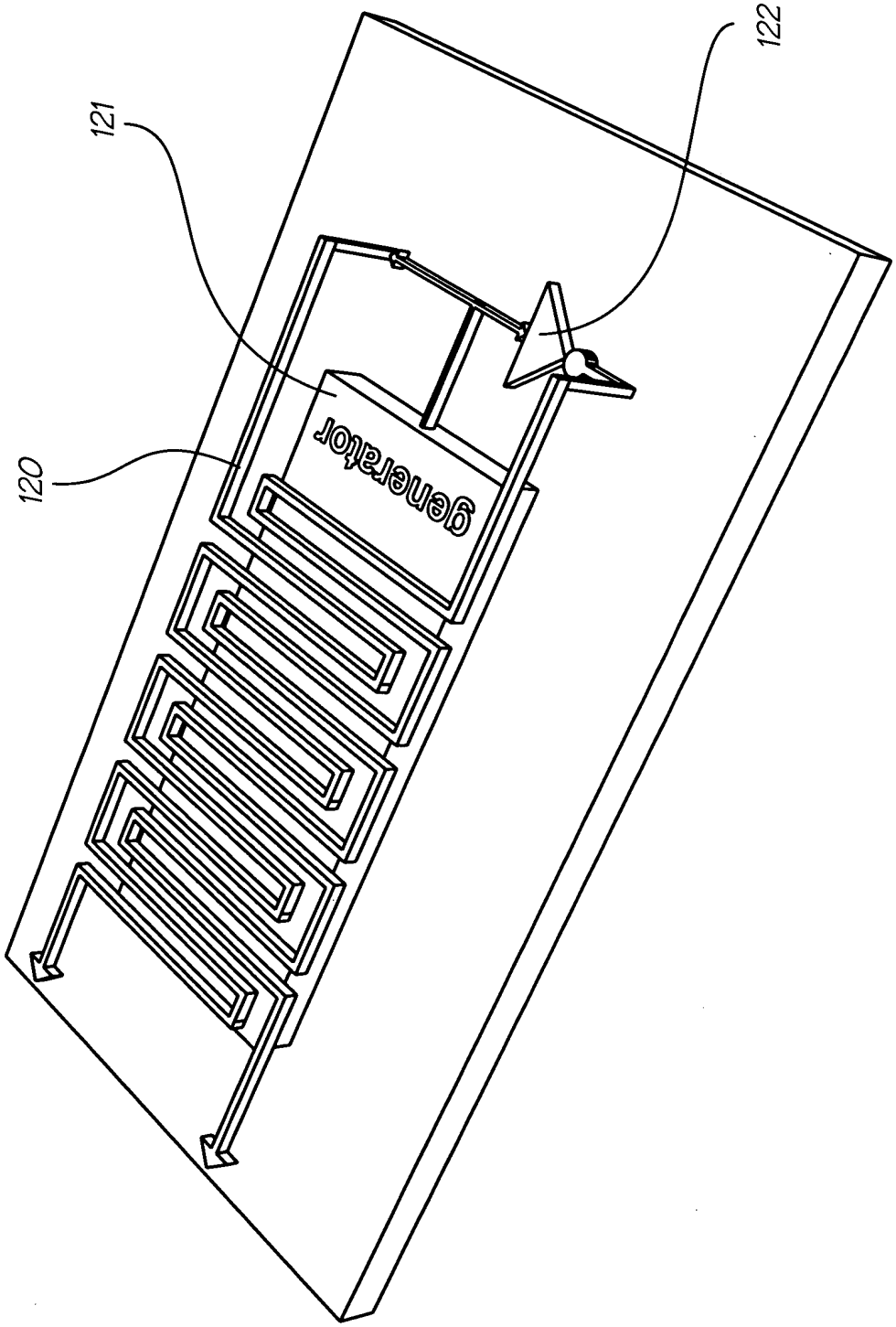

FIG. 12

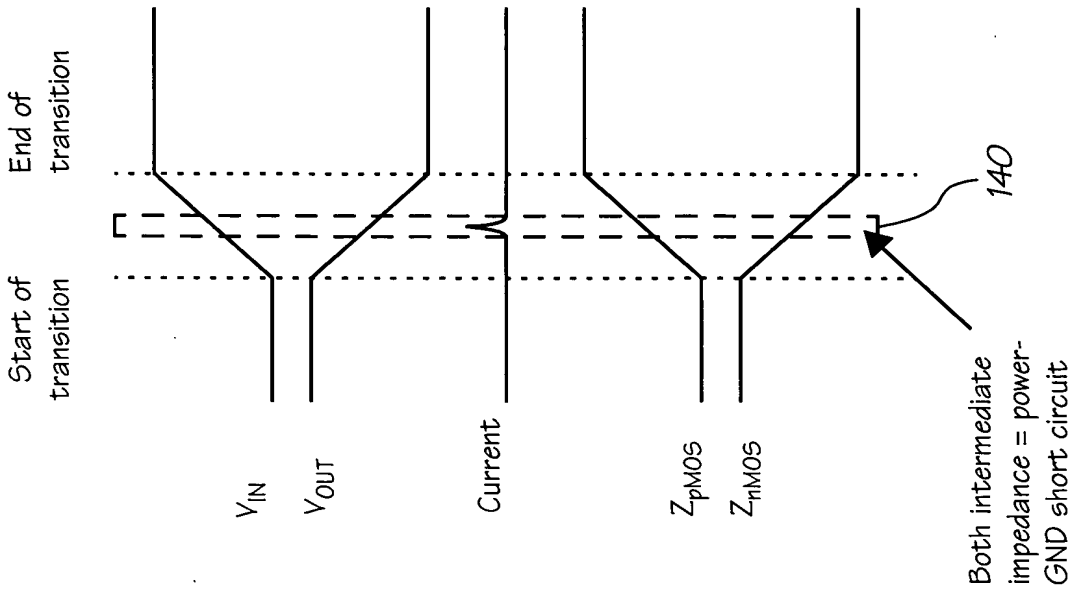
Start of transition
End of transition
V_{IN}
V_{OUT}
Current
Z_{pMOS}
Z_{nMOS}
140
Both intermediate impedance = power-GND short circuit

FIG. 14

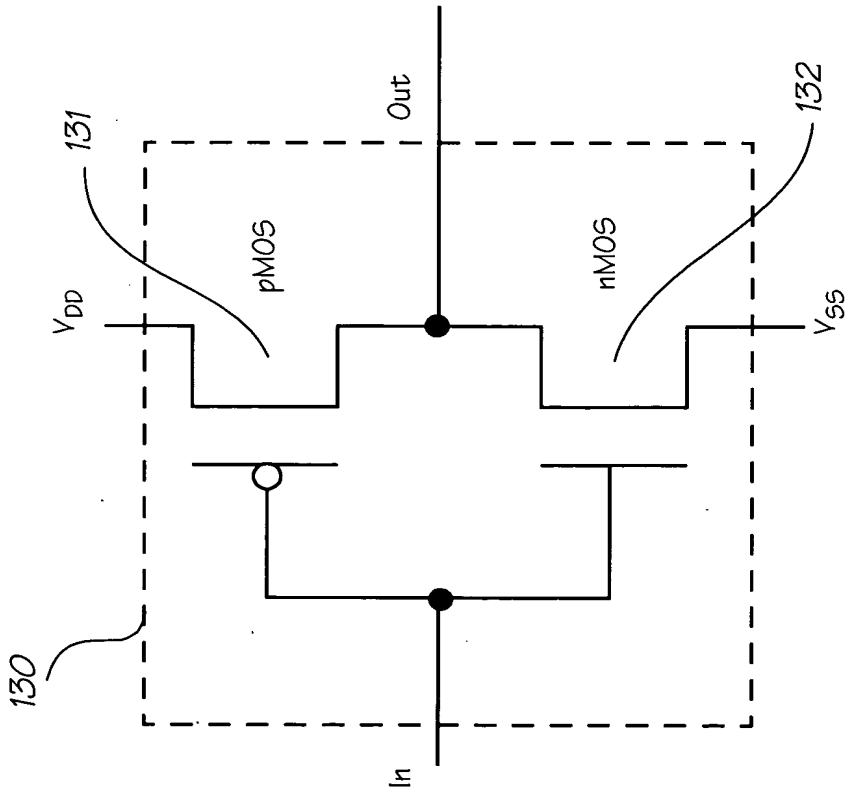
130
131
132
V_{DD}
V_{SS}
pMOS
nMOS
Out
In

FIG. 13

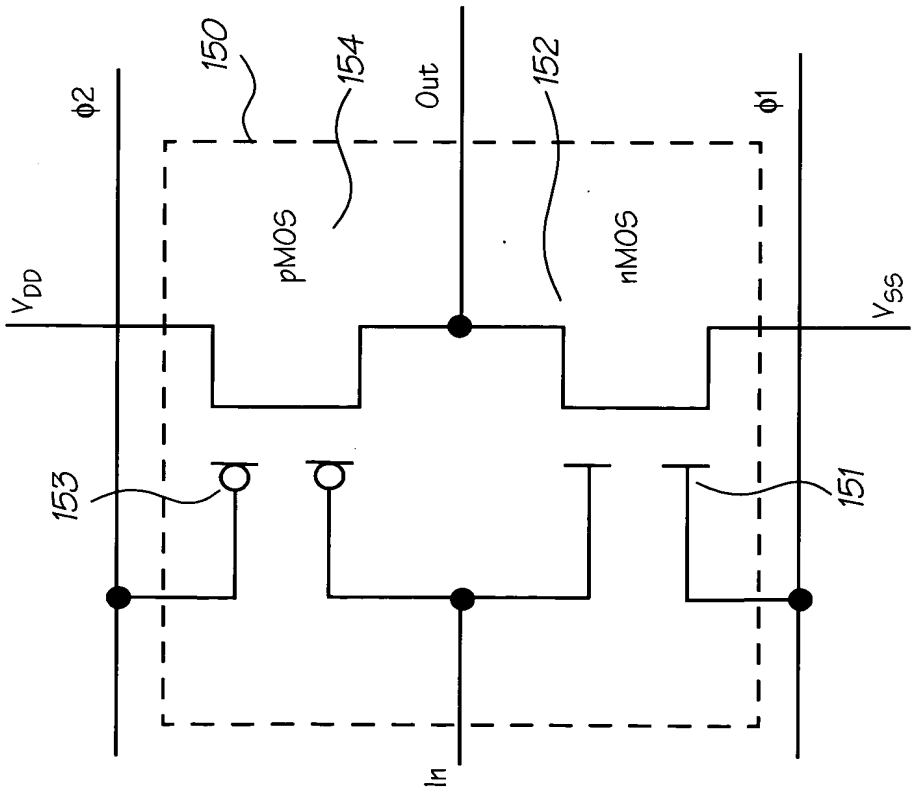
150
154
Out
152
φ2
φ1
pMOS
nMOS
V_{DD}
V_{SS}
153
151
In

FIG. 15

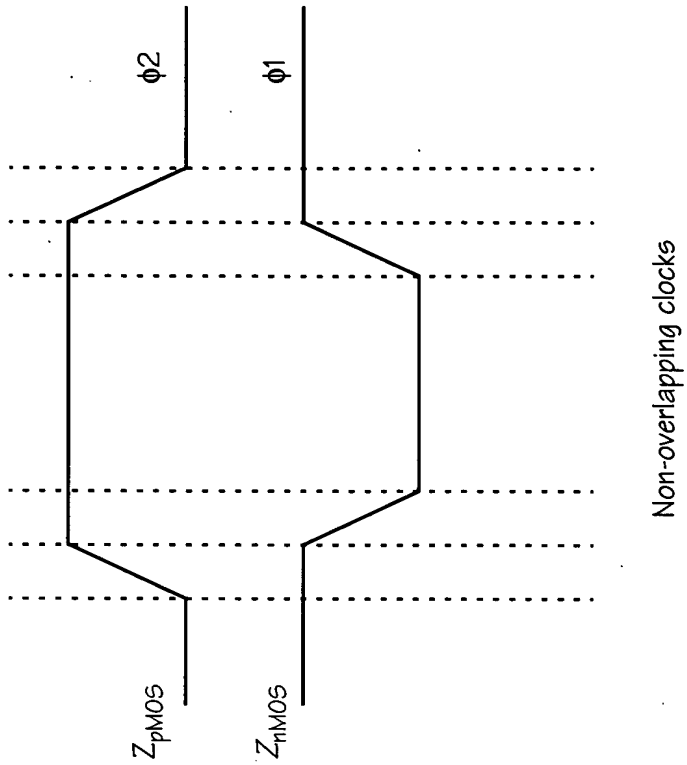
φ2
φ1
Z_{pMOS}
Z_{nMOS}
Non-overlapping clocks

FIG. 16